PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-276345
(43)Date of publication of application : 06.12.1991

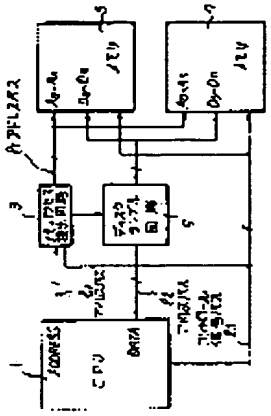
(51)Int.Cl. G06F 12/14
G06F 15/78

(21)Application number : 02-077446
(22)Date of filing : 27.03.1990

(71)Applicant : TOSHIBA CORP
TOSHIBA MICRO ELECTRON KK
(72)Inventor : SAITO YASUO

(54) MICROCONTROLLER

(57)Abstract:
PURPOSE: To prevent the decoding and the alteration of programs and data by decoding the ciphered program data stored in a memory via a descrambling means and actuating a CPU based on the decoded program data.
CONSTITUTION: A CPU 1 performs the control via an address bus signal I1 and a control signal I3 so as to send the cipher decoding key data stored in a memory 7 to a descrambling circuit 9. Then a memory access detection circuit 3 detects an access applied to a memory 5 from the CPU 1 and sends a detec tion signal to the circuit 9. Thus the circuit 9 is set in an enable state and inverts the data Di kept on a data line. The descrambled data are sent to the CPU 1 and executed there. Thus it is possible to attain a system having high security.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3−276345

⑤Int. Cl.⁵	識別記号	庁内整理番号
G 06 F 12/14	320 B	7165−5B
15/78	510 F	7530−5L

⑬公開　平成3年(1991)12月6日

審査請求　有　請求項の数 1　(全4頁)

⑭発明の名称　マイクロコントローラ

⑳特　願　平2−77446
㉒出　願　平2(1990)3月27日

⑫発明者　斎藤　靖夫　神奈川県川崎市川崎区駅前本町25番地1　東芝マイクロエレクトロニクス株式会社内
⑪出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地
⑪出願人　東芝マイクロエレクトロニクス株式会社　神奈川県川崎市川崎区駅前本町25番地1
⑭代理人　弁理士　佐藤　一雄　外3名

明　細　書

1．発明の名称

マイクロコントローラ

2．特許請求の範囲

プログラムデータが反転の暗号をかけられた状態で格納される第1のメモリと、この第1のメモリに格納されるプログラムデータにかけらる暗号を解読するのに必要なキーデータが格納される第2のメモリと、前記第1及び第2のメモリにデータを書き込んだり、読み込んだりすることを制御するCPUと、このCPUが前記第1のメモリにアクセスしているときに前記第2のメモリに格納されているキーデータに基づいて前記第1のメモリに格納されているプログラムデータにかけられている暗号を解くディスクランブル手段とを備え、前記CPUはこのディスクランブル手段によって暗号解読されたプログラムデータに基づいて動作することを特徴とするマイクロコントローラ。

3．発明の詳細な説明

［発明の目的］

（産業上の利用分野）

本発明はマイクロコントローラに関するものであって、特にセキュリティを必要とするICカードやデータバンク等に使用されるものである。

（従来の技術）

従来のマイクロコントローラにおいては、プログラムのセキュリティが考慮されておらず、メモリに記憶されたプログラムによって直接マイクロコントローラが動作していた。

（発明が解決しようとする課題）

このようなマイクロコントローラにおいては、メモリに記憶されたプログラムの解読や改ざんが容易にできるため、ハイセキュリティが要求されるICカードや、データバンクに使用するにはあまり具合のいいものではなかった。

本発明は上記事情を考慮してなされたものであって、プログラムやデータの解読や改ざんを可及的に阻止することのできるマイクロコントローラ

を提供することを目的とする。

［発明の構成］

（課題を解決するための手段）

本発明のマイクロコントローラは、プログラムデータの一部が反転の暗号をかけられた状態で格納される第１のメモリと、この第１のメモリに格納されるプログラムデータにかけらる暗号を解読するのに必要なキーデータが格納される第２のメモリと、第１及び第２のメモリにデータを書き込んだり、読み込んだりすることを制御するＣＰＵと、このＣＰＵが第１のメモリにアクセスしているときに第２のメモリに格納されているキーデータに基づいて第１のメモリに格納されているプログラムデータにかけられている暗号を解くディスクランブル手段とを備え、ＣＰＵはこのディスクランブル手段によって暗号解読されたプログラムデータに基づいて動作することを特徴とする。

（作　用）

このように構成された本発明のマイクロコントローラによれば、第２のメモリに格納されているキーデータに基づいて第１のメモリに格納されている暗号のかけられたプログラムデータがディスクランブル手段によって解読され、この解読されたプログラムデータに基づいてＣＰＵが動作する。これにより本発明のマイクロコントローラはプログラム等の解読や改ざんを可及的に阻止することができ、セキュリティの高いシステムを構築することができる。

（実施例）

第１図に本発明によるマイクロコントローラの一実施例の構成を示す。この実施例のマイクロコントローラはＣＰＵ１と、メモリアクセス検出回路３と、メモリ５，７と、ディスクランブル回路９とを備えている。メモリ５にはメインプログラムがスクランブル、すなわちデータの一部が反転の暗号をかけられた状態で格納されている。メモリ７はメモリ５のデータにかけられている暗号を解読するのに必要なキーとなるデータが格納されている。メモリアクセス検出回路３はＣＰＵ１からアドレスバスℓ１を介して送られてくるアドレス信号及びℓ３を介して送られてくるコントロール信号に基づいてＣＰＵ１がメモリ５をアクセス中であることを検出する。ディスクランブル回路９はメモリ７に格納されているキーデータに基づいてＣＰＵ１によってアクセスされているメモリ５のデータをディスクランブル、すなわち暗号を解く処理を行う。このディスクランブル回路９の一具体例を第２図に示す。この具体例のディスクランブル回路９はキーデコーダ２１と、メモリ５に格納されたｎビットのプログラムコード又はデータコードＤｏ～Ｄｎの各ビットデータＤｉ（ｉ＝１，…ｎ）のデータラインに対して設けられる暗号解読回路Ｓｉ（ｉ＝１，…ｎ）とを有している。又、暗号解読回路Ｓｉはフリップフロップ（Ｆ／Ｆともいう）Ｆと、２個のＡＮＤ回路及び２個のＮＯＲ回路からなるデータ反転回路ＩＮＶとからなっている。

次に、本実施例の作用を第１図及至第３図を参照して説明する。まずメモリ７に格納されている暗号解読のキーデータがディスクランブル回路９に送られるようにアドレス信号バスℓ１及びコントロール信号バスℓ３を介してＣＰＵ１が制御する。すると、上記キーデータはディスクランブル回路９のキーデーコーダ２１に送られてデコードされ、このデコードされた信号に基づいて暗号解読回路Ｓｉ（ｉ＝１，…ｎ）のフリップフロップＦが“１”又は“０”にセットされる（第３図ステップＦ３１、Ｆ３２参照）。次にメモリ５をＣＰＵ１がアクセスすると、これをメモリアクセス検出回路３が検出し、検出信号をディスクランブル回路９に送る（第３図ステップＦ３３参照）。するとディスクランブル回路９がイネーブル状態になる（第３図ステップＦ３４参照）。この時、フリップフロップＦが“１”にセットされた暗号解読回路Ｓｉにおいては、データ反転回路ＩＮＶのイネーブル信号が“１”となってこの暗号解読回路Ｓｉに接続されたデータライン上のデータＤｉの反転処理が行われ、フリップフロップＦが“０”にセットされた暗号解読回路Ｓｊにおいては、この暗号解読回路Ｓｊに接続されたデータラ

イン上のデータＤｊの反転処理が行われない（第３図ステップＦ３５参照）。このようにディスクランブルされたデータD'_1～D'_nはＣＰＵ１に送られて実行される。なお、ＣＰＵ１がメモリ７をアクセスするときはディスクランブル回路全体がディスエイブル（ｄｉｓａｂｌｅ）になり、データはディスクランブルされずにメモリ７上のデータはそのままＣＰＵ１に送られる。

以上述べたように本実施例によれば、メモリ５に格納されてスクランブルされたプログラム又はデータは、メモリ７に格納されているキーデータを用いてディスクランブル回路９によって暗号解読され、この暗号解読されたプログラム又はデータによってＣＰＵ１が動作する。これにより本実施例のマイクロコントローラはプログラム又はデータの解読や改ざんを可及的に阻止できるものとなる。

更に、何種類かの暗号解読のキーデータをメモリ７に格納しておけば、ひつのプログラムに何種類もの暗号をかけることができるので第３者による暗号解読を一層困難なものとすることができる。

又、ハードウェアで設計されているディスクランブル回路をソフトウェアで自由に操作できるので、ソフトウェアにかけられる暗号の種類に合せてハードを変更する必要がない。更に暗号解読のキーデータはハードウェアを変更することなく、ソフトウェアで決定することが可能となり、これによりソフトウェア設計者が暗号解読のキーデータをハードウェア設計者に知らせることなしに決定することができ、セキュリティが高く、しかも凡用性のあるシステムを実現することができる。

［発明の効果］

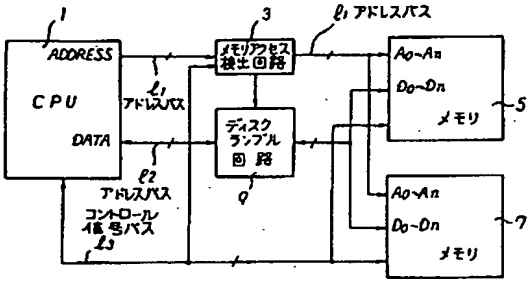
本発明によれば、プログラムやデータの解読や改ざんを可及的に防止することができ、セキュリティの高いシステムを構築することができる。

４．図面の簡単な説明

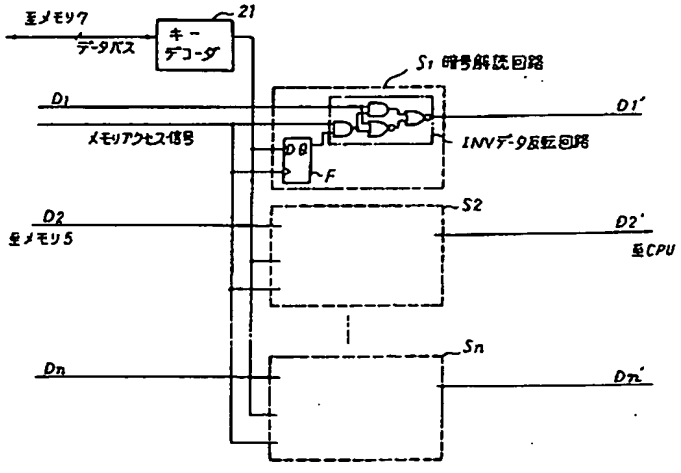
第１図は本発明のマイクロコントローラの一実施例の構成を示すブロック図、第２図は本発明にかかるディスクランブル回路の一具体例を示す回路図、第３図は実施例の作用を説明するフローチャートである。

１…ＣＰＵ、３…メモリアクセス検出回路、５，７…メモリ、９…ディスクランブル回路。

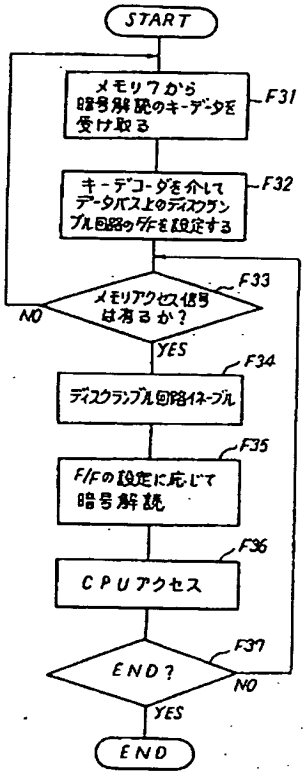
出願人代理人　佐　藤　一　雄



第１図



第２図



第3図

手続補正書

平成 3 年 1 月 16 日

特許庁長官 植松 敏 殿

1 事件の表示

平成 2 年特許願第 77446 号

2 発明の名称

マイクロコントローラ

3 補正をする者

事件との関係 特許出願人

(307) 株式会社 東芝

(ほか 1 名)

4 代理人 (郵便番号 100)
東京都千代田区丸の内三丁目2番3号
[電話東京 (3211)2321 大代表]

6428 弁理士 佐藤 一雄

5 補正命令の日付

発送日 平成 年 月 日

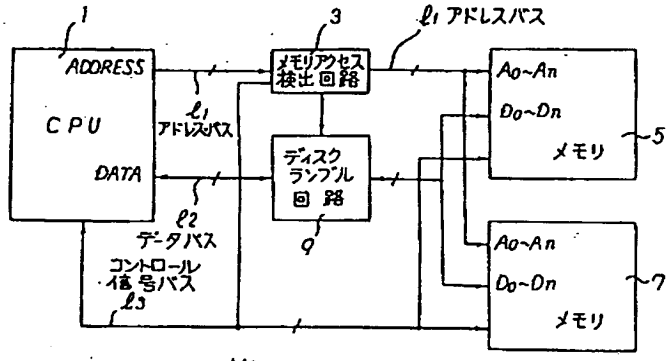
6 補正により する請求項の数

7 補正の対象

図面

8 補正の内容

図面中、第1図を別紙の通り訂正する。



第1図